

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA

09 Cr. 1037

v.

OPINION

PATRICK NAYYAR,

Defendant

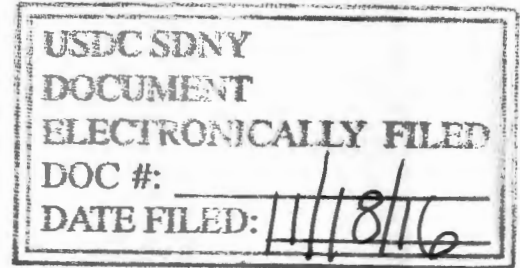
-----X

A P P E A R A N C E S:

Counsel for Government  
UNITED STATES ATTORNEY'S OFFICE  
Southern District of New York  
One St. Andrew's Plaza  
New York, NY 10007  
By: Sean S. Buckley, Esq.

UNITED STATES ATTORNEY'S OFFICE  
Southern District of New York  
300 Quarropas Street  
White Plains, NY 10601  
By: Stephen J. Ritchin, Esq.

Counsel for Defendant  
COOLEY LLP  
1114 Avenue of the Americas  
New York, NY 10036  
By: Laura Grossfield Burger, Esq.



**Sweet, D.J.**

This action was remanded by the Second Circuit Court of Appeals to conduct a hearing with respect to computer evidence received at trial. Upon the facts and conclusions set forth below, the computer evidence will not be suppressed.

### **I. Prior Proceedings and Facts**

In July 2009, the Federal Bureau of Investigation ("FBI") began an investigation of defendant Patrick Nayyar ("Nayyar" or the "Defendant") that focused on Nayyar's offers to sell to Hizballah military-grade weapons and supplies, including sniper rifles, armor-penetrating sniper bullets, Uzis, night-vision goggles, and bullet-proof vests. The investigation further involved Nayyar's sale of a handgun, hollow-point bullets, and a truck to a man Nayyar thought was acting on behalf of Hizballah, but who was actually a confidential informant ("CI") working for the FBI. See Factual Stipulation by the Parties (June 6, 2016) [hereinafter "Stip."] Ex. G ¶¶ 8-9. More than a dozen meetings between Nayyar and the CI were recorded by the FBI; those meetings lasted, in total, about 20 hours. See Trial Transcript (March 19-23, 2012) [hereinafter

"Tr."] 12. During the investigation, Nayyar provided the CI with an arms catalog, which contained descriptions and specifications for weapons ranging from high-powered rifles to rocket-propelled grenades, printouts of specifications for M-18 mines and night-vision goggles, and an armor plate for use in bulletproof vests. Government Trial Exhibit [hereinafter "GX"] 3, GX 48, GX 53, GX 61.

On September 24, 2009, Nayyar was arrested at his apartment in Queens. Stip. ¶ 1. Nayyar's wife, who also lived in the apartment, consented to a search of the apartment. Stip. ¶¶ 3-4. During the search, FBI agents located two laptop computers, one of which Nayyar's wife told the agents that she typically used. The other, which the agents had found on a bookshelf in the hall of the apartment, Nayyar's wife told the agents Nayyar typically used. Stip. ¶¶ 6-8.

The agents took Nayyar's computer with them after Nayyar's wife consented to the search of that computer, provided the agents with a password for it, and signed a consent-to-search form which described both computers as ones "which I own, possess, control and/or have access to." Stip. ¶¶ 8-9. Nayyar's wife did not volunteer any information about whether it was a

current password she had provided or when she had last used the computer, nor did the agents ask her about those subjects. Stip. ¶ 8.

On October 26, 2009, Nayyar was indicted for conspiring to provide, and providing, material support to Hizballah; conspiring to make, and making, a contribution of funds, goods or services to Hizballah; and illegal possession of a firearm and ammunition. See Indictment.

The computer the FBI had seized was subsequently provided to the FBI's Computer Analysis Response Team ("CART") for examination. Stip. ¶ 12. FBI Special Agent Candace Hunter ("Agent Hunter"), the CART agent assigned to the task, reviewed a copy of Nayyar's wife's consent to search the computer and then created a forensic image of the computer to permit review by the case agents. Stip. ¶¶ 15-16. The software used to create the forensic image did not require the use of a password.

Review began on December 18, 2009, when FBI Special Agent Michael Kelley ("Agent Kelley"), looking to obtain evidence related to a printout about night-vision goggles that Nayyar had provided to the CI, conducted searches for "night

vision goggles" and "M-16." Stip. ¶ 23(a)-(d). Agent Kelley created three bookmarks labeled "Graphics of Interest," in which he placed files. Stip. ¶ 23(e)-(j). Because the forensic imaging did not require a password, Agent Kelley did not then know whether the password provided by Nayyar's wife worked. Stip. ¶ 24(d)-(e). Agent Kelley's review of the computer lasted from 11:18 a.m. until 12:36 p.m.; it was halted after he identified images that he suspected might be child pornography. Stip. ¶ 23.

On December 21, 2009, Agent Kelley spoke with Assistant U.S. Attorney Sean Buckley ("AUSA Buckley"). Stip. ¶ 24. Upon learning that Agent Kelley did not know whether the password the FBI had obtained from Nayyar's wife worked to unlock the computer, AUSA Buckley instructed Agent Kelley to find out whether Nayyar's wife had access to the computer and knew its password. *Id.* Nayyar's wife then told Agent Kelley that before the summer of 2009 she had access to the computer and knew its password, but after she found pornography on the computer in August 2009 and confronted Nayyar about her discovery, he changed the password and did not tell her the new password. Stip. ¶ 25(a).



When Agent Kelley reported this conversation to AUSA Buckley, AUSA Buckley told Agent Kelley not to conduct any further review of the computer, and expressed concerns about the consent to search the computer that Nayyar's wife had provided. Stip. ¶ 25(b). AUSA Buckley also told Agent Kelley that the FBI should obtain a search warrant for the computer in order to cure any potential deficiency in the consent from Nayyar's wife that the FBI had relied on to begin the review of the computer. *Id.* AUSA Buckley further told Agent Kelley that once the warrant was obtained, if the FBI identified confirmed images of child pornography on the computer, the FBI would need to obtain a new search warrant specific to child pornography. *Id.* Agent Kelley was walled off from the search warrant application, which contained no information obtained during the initial search of the computer. Stip. ¶ 31.

FBI review of the computer began again on November 8, 2010, shortly after a magistrate judge issued a search warrant for the computer. Stip. ¶¶ 33, 35. The form signed by Nayyar's wife consenting to the search of the computer had been provided to the defense two months prior, on September 1, 2010. Stip. ¶ 8. On March 16, 2011, Agent Hunter prepared an electronic version of a report setting forth each of the steps she had

taken on the computer and the forensic image of the computer. Stip. ¶ 23(f), n.3. This report, called the FTK Report, included the items bookmarked by the case agent as "Graphics of Interest." *Id.*; Stip. ¶ 23(f), n.4-5. The FTK Report also included an "Evidence List," which identified the five partitions on the computer that were the subject of the FTK Report, and stated that each partition was added to the review program used to analyze the computer on December 2 or 3, 2009. Stip. ¶ 53.

On March 22, 2011, and again on February 24, 2012, a copy of the FTK Report was made available to Nayyar's defense counsel. Stip. ¶ 53, 54. Copies of Agent Hunter's Jencks Act material, including her Communications Log, which contained dated entries of communications she had in connection with her examination of the computer, and her Examination Notes, which contained notes she took of steps taken in the course of her forensic examination of the computer, were provided to the defense on Wednesday, March 14, 2012, five days before the start of trial. Stip. ¶ 13, 14. Nayyar made no motion seeking to suppress the computer or evidence from it prior to trial.

Trial began on March 19, 2012. The Government's proof consisted primarily of: (i) recordings of Nayyar's many conversations with the CI; (ii) the items that Nayyar sold to the CI; (iii) documents that Nayyar provided to the CI in connection with negotiations, such as a catalog from a weapons manufacturer, a copy of the title for the truck that Nayyar sold to the CI believing that it would be shipped to Hizballah, and print-outs of specifications for night-vision goggles, M-18 anti-personnel mines, and a Russian made helicopter; (iv) admissions that Nayyar made during a post-arrest interview with the FBI and then during a proffer with the Government; and (v) items recovered during a search of Nayyar's home and his mother's home, including several boxes of ammunition and an arms catalog. In addition, the Government offered proof obtained from a search of the computer that demonstrated that the computer had accessed several websites that described military-grade items like bulletproof vests, and had also accessed a newspaper article that described Hizballah as a terrorist organization. See Tr. 72-74, 79-82, 92-97; GX 25E.

At trial, Agent Hunter testified that she processed the hard drive that was obtained from the computer in order to prepare the hard drive's contents for review. Tr. 58-60. She



also testified that she "started [her] examination of the computer" on "December 2 of 2009." Tr. 105. Her testimony concluded in the morning of the second day of trial. Tr. 106. The next morning, before the jury was called in to begin the third day of trial, Nayyar's counsel moved for a mistrial. Tr. 190-91. As the basis for the motion, defense counsel explained that the computer evidence introduced through Agent Hunter should have been suppressed as the fruit of a warrantless search because "the search warrant for the computer was not . . . signed off on until October 29th of 2010," and Agent Hunter's trial testimony had revealed to the defense for the first time that Agent Hunter had already "searched the computer . . . in December of 2009." *Id.*

The Government responded with three reasons why the computer evidence was not suppressible and, accordingly, why the mistrial motion should be denied. First, Nayyar had not moved to suppress the computer evidence prior to trial despite notice of the computer's search, and so "any suppression motion ha[d] been waived." Tr. 192. Second, any search of Nayyar's computer that had occurred prior to obtaining the search warrant was based on written consent provided by Nayyar's wife, who had "at the very least apparent authority" to authorize a search. *Id.* Third, when

a question subsequently arose concerning Nayyar's wife's authority to give consent, the Government "walled off" the case agent who had begun the search and obtained a search warrant "based upon facts that existed well in advance of the December 2009 processing of the computer." *Id.*

The defense responded, and the Court agreed, that the scope of Agent Hunter's pre-warrant activities presented a "factual issue." Tr. 195. The Court suggested recalling Agent Hunter to testify on the issue outside the presence of the jury. *Id.* The Government reported that Agent Hunter had left town, and said that bringing her back was unnecessary because, irrespective of what she had done in processing the computer in 2009, the defendant's motion failed on the waiver ground and the fact that the Government had obtained a search warrant based on information independent of anything learned from the computer. The Government framed the issue as one of inevitable discovery. Tr. 195-97.

The Court indicated that the fact of the independently-obtained search warrant was probably dispositive, but declined to rule without further information. Tr. 197. Instead, the Court (i) invited the defense to make a written

submission, and (ii) directed the Government to report back with a "factual recital" about the relevant events, so that the Court and the parties could "see if there is anything that is contentious about [the facts] and what it is." Tr. 197-98.

The Government then provided a proffer of what Agent Hunter would say. After additional argument, the Court denied Nayyar's mistrial motion, finding that any challenge to the computer evidence "ha[d] been waived" because Nayyar did not move to suppress the evidence prior to trial even though it had been clear that "the computer obviously had been seized" and "there was a consent to search granted by Mr. Nayyar's wife." Tr. 232-33. In addition, and in any event, the Court accepted the Government's argument that the doctrine of inevitable discovery defeated any suppression motion because the Government had obtained a search warrant based on evidence that was independent of any purportedly unauthorized search of the computer. Tr. 233.

On March 27, 2012, Nayyar was convicted of all counts. Tr. 737-38. On October 27, 2014, he was sentenced principally to 15 years' imprisonment.

Nayyar argued on appeal that this Court's denial of his motion for a mistrial was error because he did not waive his Fourth Amendment rights, the FBI did not receive valid consent to search the computer, the FBI conducted illegal searches of the computer before obtaining a warrant and the inevitable discovery and independent source doctrines did not apply. Nayyar also argued that there was insufficient evidence to support his conviction for engaging in a conspiracy to traffic in guns and ammunition.

On October 14, 2015, the Court of Appeals issued a summary order remanding the case to this Court "to conduct a post-trial hearing on the issues relating to the computer evidence received at trial." *United States v. Mulholland*, 628 F. App'x 40, 42 (2d Cir. 2015) (summary order). Specifically, the Court of Appeals remanded for the Court to conduct a hearing on "whether (1) Nayyar waived his right to challenge the evidence in question, (2) Nayyar's wife's consent was valid, and (3) the independent source doctrine applies." *Id.* at 43.

Since the Second Circuit's decision, as Nayyar notes in his Memorandum of Law in Connection with Proceedings on Remand (June 17, 2016) [hereinafter "Nayyar Br."] at 5, the

Government conducted further inquiry into the facts surrounding the computer search, and shared those facts with the defense. The parties have entered into a 23-page stipulation of facts, with numerous exhibits attached, which, in the view of the parties and the Court, has obviated the need for an evidentiary hearing.

The hearing was completed and argument heard on September 22, 2016.

## **II. Nayyar Waived His Right to Challenge the Computer Evidence**

Rule 12 of the Federal Rules of Criminal Procedure provides that a motion to suppress evidence must be made before trial. See Fed. R. Crim. P. 12(b)(3)(C). Thus, a suppression motion that is not made before trial "is untimely," and may not be considered unless "the party shows good cause." Fed. R. Crim. P. 12(c)(3); *see also United States v. Gonzalez*, 764 F.3d 159, 170 (2d Cir. 2014) ("Appellant did not move to suppress the identification and thus waived this issue."); *United States v. Yousef*, 327 F.3d 56, 125 (2d Cir. 2003) ("[W]e will find complete waiver of a suppression argument that was made in an



untimely fashion before the district court unless there is a showing of cause." ).

Analysis of whether a suppression claim has been preserved focuses not on whether the evidence was challenged on some ground, but whether the particular ground for suppression pressed later could have been, but was not, advanced prior to trial. See *United States v. Klump*, 536 F.3d 113, 120 (2d Cir. 2008) ("It is well-settled that the failure to assert a particular ground in a pre-trial suppression motion operates as a waiver of the right to challenge the subsequent admission of evidence on that ground.") (internal quotation marks and citation omitted); *United States v. Rollins*, 522 F.2d 160, 165 (2d Cir. 1975) ("[T]he failure to assert before trial a particular ground for a motion to suppress certain evidence operates as a waiver of the right to challenge the admissibility of the evidence on that ground." ).

There is no dispute that Nayyar was made aware well before trial that his wife had consented to the search of the computer at issue. See Nayyar Br. at 20; Government's Memorandum of Law in Connection with Remand Proceedings (July 15, 2016) [hereinafter "Gov't Br."] at 33. Likewise, there is no dispute

that Nayyar never challenged the validity of his wife's consent prior to the commencement of trial. Rather, Nayyar contends that his failure to challenge that consent should be excused because he "had good cause for not challenging the search prior to trial." *Id.*; see also *United States v. Sanchez*, 813 F. Supp. 241, 249 (S.D.N.Y. 1993) ("[I]t is clear that where the grounds for the motion are not discoverable by the defendant until after the trial has begun, cause is established.").

Specifically, Nayyar argues that he "had no reason to challenge the validity of his wife's consent prior to trial" because the Government represented at a 2010 court conference that it would be getting a search warrant and Nayyar was unaware that some searches had already occurred. *Id.* at 29-30; see also Nayyar's Reply Memorandum of Law in Connection with Proceedings on Remand (July 29, 2016) [hereinafter "Nayyar Reply Br."] at 9-10. While the Government argues that Nayyar was put "on notice" by the provision of certain evidence before trial, Gov't Br. at 33, Nayyar asserts that "it was not until Agent Hunter's testimony that the defense became aware of the basis for a motion." Nayyar Br. at 20. As set forth below, the basis for the motion was presented to and discoverable by the Defendant prior to that time.

The computer was seized by the FBI on September 24, 2009, and the initial consent to search the computer was provided that same day. A copy of the signed consent form, as well as a list of materials seized, was provided to the defense on September 1, 2010. Stip. ¶ 8; see also Tr. 190 (defense counsel's acknowledgment that "[t]he computer information was turned over . . . a long time ago"); Tr. 231 (defense counsel's acknowledgment that "the consent to search form . . . is in the discovery"); Tr. 232-33 (District Court's observations during trial that "the computer obviously had been seized," and that "there was a consent to search granted by Mr. Nayyar's wife" supported finding of waiver). On March 22, 2011, the Government provided the Defendant with the FTK Report, from which the Defendant could see that that the FBI had begun looking at the contents of the computer in December 2009. See Stip. ¶ 54 (stating that counsel for the Defendant "confirmed that he had received evidence obtained from the defendant's hard drive," i.e., the FTK Report). Thereafter, on February 24, 2012, the Government re-produced the FTK Report, which again included the aforementioned Evidence List. On March 4, 2012, defense counsel confirmed in writing that "he was able to review" the contents of the FTK Report. Stip. ¶ 58.

The crux of Nayyar's argument on remand is that, though he and his counsel received the FTK report created by Agent Hunter on March 22, 2011 - nearly one year prior to the commencement of Nayyar's trial - the information contained therein did not make clear that pre-warrant searches had been conducted on the computer. Nayyar Reply Br. at 9-10. Nayyar argues that the FTK Report "does not show the dates or times" when the FBI performed its review of the forensic image. Nayyar Br. at 17. To the contrary, the third item on the FTK Report, a document entitled "Evidence List," specified that each of the five portions of Nayyar's computer that were reviewed by the FBI were added to the FTK AccessData review program on either December 2 or 3, 2009. Gov't Br. at 35. Nayyar further argues that that the indication files were "added" to the FTK review program does not make clear that those files were reviewed. Nayyar Reply Br. at 9.

Prior to the trial in this case, however, the Government also provided early disclosure of Jencks Act materials. On March 14, 2012 - five days before trial - the Government provided Jencks Act materials that related to Agent Hunter's anticipated testimony. Gov't Br. at 35. Three of the documents contained within Agent Hunter's Jencks Act materials -



which were comprised of a total of only 13 documents<sup>1</sup> - explicitly stated that the examination of the computer commenced in 2009. First, the CART Request Summary (3503-8), which was created on November 2, 2009, requested that a "full examination" be conducted of the laptop and further indicated that the computer had been assigned to a CART examiner on November 25, 2009. See Stip., Ex. C. Second, Agent Hunter's Communications Log stated that Agent Hunter commenced her examination on December 2, 2009, and that Agent Kelley started and terminated his substantive review of the computer on December 18, 2009. See Stip., Ex. D. Third, Agent Hunter's "Examination Notes" set forth in great detail each and every step Agent Hunter took with respect to the computer, which establish that Agent Hunter and the FBI relied upon the "signed consent to search form for a laptop computer." See Stip., Ex. E.

Only a challenge to the validity of Nayyar's wife's consent to search the computer could call into question the legality of the FBI's search, and such a challenge was - as the Court previously found - waived by Nayyar when he chose not to

---

<sup>1</sup> Nayyar has contended that he would have had to "scour all of the \$ 3500 material" in order to determine that a search had occurred prior to the issuance of the warrant. Nayyar Br. at 21. As indicated above, Agent Hunter's Jencks Act materials consisted of only 13 documents, which spanned a total of 44 pages. And three of those 44 pages showed that a search was commenced in December 2009. Gov't Br. at 36, n.7.



mount it prior to trial. See *Klump*, 536 F.3d at 120; Tr. 232-33. The provision to the Defendant of documents showing the 2009 computer review contradict his claim that "[i]t was not until Agent Hunter testified at Nayyar's trial that it became clear that the FBI had conducted searches of the laptop without entering the password and prior to getting the warrant." Nayyar Br. at 21. The first production of the consent-to-search form in September 2010, the production of the FTK Report in March 2011, its re-production in February 2012, and Agent Hunter's Jencks Act materials shortly before the commencement of trial certainly when taken together provided Nayyar with the information to move to suppress the 2009 searches prior to trial should he have wanted to do so.

The motion to suppress was untimely, not for good cause, and was therefore waived.

### **III. The Consent of Mrs. Nayyar Was Not Valid Under Actual or Apparent Authority**

The Government does not contend that Mrs. Nayyar had actual authority to agree to the computer search, but rather that the agents appropriately relied on her apparent authority.

While the reliance appeared to be reasonable, under all the circumstances presented here, further inquiry at the time of seizure was required to eliminate any ambiguity as to authority. The failure to investigate further in this instance bars the reliance on apparent authority.

"[W]hen the prosecution seeks to justify a warrantless search by proof of voluntary consent, it is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." *United States v. Matlock*, 415 U.S. 164, 171 (1974) (footnote omitted). "A third party has actual authority to provide consent to search if 'first, the third party had access to the area searched, and second, either: (a) common authority over the area; or (b) a substantial interest in the area; or (c) permission to gain access.'" *United States v. Marandola*, 489 F. App'x 522, 523 (2d Cir. 2013) (summary order) (quoting *United States v. Davis*, 967 F.2d 84, 87 (2d Cir. 1992)).

Even if the party providing consent lacked actual authority, "a warrantless entry is valid when based upon the

consent of a third party whom the police, at the time of the entry, reasonably believe to possess common authority over the premises." *Illinois v. Rodriguez*, 497 U.S. 177, 179 (1990). In other words, in the absence of actual authority, law enforcement may rely upon apparent authority so long as the reliance is not "unrealistic." See *id.* at 187-88. The test is an objective one: If "the facts available to the officer at the moment . . . warrant a man of reasonable caution in the belief that the consenting party had authority over the premises," then the search is valid. *Id.* at 188 (internal quotation marks and citation omitted); see *United States v. Sparks*, 287 F. App'x 918, 920 (2d Cir. 2008) (same).

Here, permission to search the computer was given by Nayyar's wife, who lived with him in the apartment where the computer was found. Stip. ¶¶ 3, 8. The computer was found in a commonly accessible space, a bookshelf in the hall of the apartment. Stip. ¶ 7. Nayyar's wife signed a form which described the computer as one "which I own, possess, control and/or have access to." Stip., Ex. B. But Nayyar's wife orally described the computer as one that Nayyar, not she, "typically used" and which had a password. She provided a password for the computer to the FBI but did not mention that it was outdated.

Stip. ¶ 8. That password was recorded on the consent to search form that she signed. Stip., Ex. B.

Nayyar had changed the password for the computer during the month prior to the search, and had not shared the new password with his wife. See Stip. ¶ 25(a). However, "at the time of entry," *Rodriguez*, 497 U.S. at 179, i.e., the time the FBI began to search, the FBI did not know about that change in Nayyar's wife's access to the computer. The Government relies on the facts that Mrs. Nayyar told the FBI agents that Nayyar "typically used" the laptop rather than stating that it did not belong to her and that the laptop was found in a common area in their home accessible to Mrs. Nayyar.

In the event of ambiguity as to the scope of authority over the laptop, the agents were required to ask further questions regarding the scope of her purported authority to consent before relying on it. See *United States v. Purcell*, 526 F.3d 953, 963-64 (6th Cir. 2008) ("[A]pparent authority cannot exist if there is ambiguity as to the asserted authority and the searching officers do not take steps to resolve the ambiguity."). The "facts available to the officer[s] at the moment," *Rodriguez*, 497 U.S. at 188, may have initially pointed



to Mrs. Nayyar's apparent authority, but especially because Mrs. Nayyar distinguished between her "typically used" laptop and Nayyar's "typically used" laptop, and the agents seized only Nayyar's laptop, the officers should have inquired further. See *Sparks*, 287 F. App'x at 920 (finding valid apparent authority where the driver of a car consented to the search of his passenger's bag while noting that "[t]he reasonableness of th[e] arresting officer's] belief could have been dispelled if, for example, either [the passenger] or [the driver] had indicated that the Tote Bag behind [the passenger]'s seat was his."); see also *Purcell*, 526 F.3d at 964 ("When a situation starts as unambiguous but subsequent discoveries create ambiguity, any apparent authority evaporates."). Their failure to do so precludes the Government from relying upon apparent authority here. See *United States v. Turner*, 23 F. Supp. 3d 290, 311 (S.D.N.Y. 2014) (finding that the defendant's girlfriend had apparent authority to consent to search of shared apartment, but not to search of the defendant's backpack because the police asked no "further questions" to establish her "ownership, control, or use" of the backpack); *United States v. Gonzalez Athehorta*, 729 F. Supp. 248, 257 (E.D.N.Y. 1990) (no apparent authority where the officer "opted to remain ignorant rather



than ask a few pertinent questions that could have clarified the situation").

Reliance on the boilerplate language on the consent form does not resolve the issue. The form references both laptops found in the residence, and there is no basis to conclude that the boilerplate language applied to Nayyar's laptop as opposed to hers. The language on the form does not say that Mrs. Nayyar owned or possessed either laptop; it says "own, possess, control and/or have access to." Though Mrs. Nayyar provided a password, which served as an indicia of authority, a further inquiry as to whether the password was current or when she had last used the laptop would have revealed what was later discovered: that she had been deliberately deprived of access, and the password she provided did not work.

Given the unusually intrusive nature of computer searches, confirmation of the validity of third-party consent is worth the additional time and effort even during the pressures of arrest and investigation. See *United States v. Ganas*, No. 12-240-CR, 2016 WL 3031285, at \*24 (2d Cir. May 27, 2016) (Chin, J., dissenting) ("Virtually the entirety of a person's life may be captured as [computer] data."); *United States v. Payton*, 573

F.3d 859, 861-62 (9th Cir. 2009) ("[C]omputers are capable of storing immense amounts of information and often contain a great deal of private information."); cf. *United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013) (where "property to be searched is a computer hard drive, the particularity requirement [for search warrants] assumes even greater importance" because the "potential for privacy violations . . . is enormous").

#### **IV. The Independent Source Doctrine Applies to the Admission of the Computer Evidence**

The court-created "exclusionary rule" doctrine - which requires courts to suppress evidence that is the tainted "fruit" of unlawful government conduct - and the "independent source" doctrine - which serves as an exception to the exclusionary rule - were born together. While information obtained in violation of the Fourth Amendment "does not automatically become 'sacred and inaccessible,'" if "knowledge of [such information] is gained from an independent source, they may be proved like any others." *Nix v. Williams*, 467 U.S. 431, 441 (1984) (quoting *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920)).

The independent source limitation on the exclusionary rule stems from the rationale underlying it:

The core rationale consistently advanced by this Court for extending the exclusionary rule to evidence that is the fruit of unlawful police conduct has been that this admittedly drastic and socially costly course is needed to deter police from violations of constitutional and statutory protections. This Court has accepted the argument that the way to ensure such protections is to exclude evidence seized as a result of such violations notwithstanding the high social cost of letting persons obviously guilty go unpunished for their crimes. On this rationale, the prosecution is not to be put in a better position than it would have been in if no illegality had transpired.

By contrast, the derivative evidence analysis ensures that the prosecution is not put in a worse position simply because of some earlier police error or misconduct. . . . The independent source doctrine teaches us that the interest of society in deterring unlawful police conduct and the public interest in having juries receive all probative evidence of a crime are properly balanced by putting the police in the same, not a worse, position that they would have been in if no police error or misconduct had occurred. When the challenged evidence has an independent source, exclusion of such evidence would put the police in a worse position than they would have been in absent any error or violation.

*Nix*, 467 U.S. at 442-43 (footnote and citations omitted).

Where a warrant-authorized search is preceded by a warrantless entry, the Supreme Court has explained that evidence would not be suppressed if "[n]one of the information on which the warrant was secured was derived from or related in any way to the [unlawful] entry . . . [and] the information came from

sources wholly unconnected with the entry and was known to the agents well before the [illegal] entry." *Segura v. United States*, 468 U.S. 796, 814 (1984). Where a warrant-authorized search is preceded by a warrantless search, "[t]he ultimate question [] is whether the search pursuant to warrant was in fact a genuinely independent source of the information and tangible evidence at issue []. This would not have been the case if the agents' decision to seek the warrant was prompted by what they had seen during the initial entry, or if information obtained during that entry was presented to the Magistrate and affected his decision to issue the warrant." *Murray v. United States*, 487 U.S. 533, 542 (1988) (footnote omitted).

Our Circuit explored the independent source doctrine in *United States v. Johnson*, 994 F.2d 980 (2d Cir. 1993), a case cited in the Second Circuit's remand here. In *Johnson*, the Circuit explained that the doctrine applies "in cases where the police stumble upon evidence while engaging in an unlawful search or entry, but where there was an independent basis apart from the illegal entry to allow a warrant to issue." *Id.* at 987. As the Second Circuit noted, the independent source doctrine requires that: "(1) the warrant [was] supported by probable cause derived from sources independent of the illegal[ity]; and



(2) the decision to seek the warrant [was not] prompted by information gleaned from the illegal conduct." *Id.* at 987 (citing *Murray v. United States*, 487 U.S. at 542). With regard to the second prong, the "relevant question is whether the warrant 'would have been sought even if what actually happened had not occurred.'" *Id.* (citing *Murray*, 487 U.S. at 542).

Nayyar has conceded that the first prong of the test set forth in *Murray* and *Johnson* has been satisfied. Nayyar Br. At 16, n. 8. He claims only that the search of the computer at issue pursuant to a search warrant was not independent of the earlier search - a failure to satisfy the second prong of the test. Specifically, he argues that "the Government's decision to seek a warrant was prompted by the prior review by Agent Kelley." Nayyar Br. at 15 (emphasis in original). Nayyar's logic is as follows: "It is undisputed that Agent Kelley halted his search upon encountering images he thought might be child pornography, and contacted AUSA Buckley for guidance. Had he not seen the potential child pornography, Agent Kelley's search would have continued unabated; it was the discovery of possible child pornography during the search that animated the decision to obtain a warrant." *Id.* This, according to Nayyar, "is



precisely what the second prong of the Johnson test prohibits." Nayyar Br. at 15-16.

The Supreme Court has long rejected the notion that "but-for" causation is all that is required for courts to apply the exclusionary rule. As the Supreme Court noted more than 50 years ago when the Government conceded that a statement unlawfully obtained had led it to find drugs:

We need not hold that all evidence is "fruit of the poisonous tree" simply because it would not have come to light but for the illegal actions of the police. Rather, the more apt question in such a case is "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint."

*Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963) (quoting *Maguire, Evidence of Guilt*, 221 (1959)); see *Hudson v. Michigan*, 547 U.S. 546, 592 (2006) ("exclusion may not be premised on the mere fact that a constitutional violation was a 'but-for' cause of obtaining evidence.").

Rather, the "primary evil" that the second prong of the independent doctrine test "seeks to root out is the so-

called 'confirmatory search,'" which occurs "when officers conduct a search to get assurance that evidence is present before taking the time and effort to obtain a warrant." *United States v. Hanhardt*, 155 F. Supp. 2d 840, 847-48 (N.D. Ill. 2001) (citing *Murray*, 487 U.S. at 540 n.2) (other citations omitted); *United States v. Brooks*, No. 15-CR-6157G, 2016 WL 1749394, \*6 (W.D.N.Y. May 2, 2016) (quoting *Hanhardt*); accord *United States v. Restrepo*, 966 F.2d 964, 971-72 (5th Cir. 1992) ("Murray is intended to deal with the so-called confirmatory search, conducted for the precise reason of making sure it is worth the effort to obtain a search warrant.") (internal quotations and footnote omitted). Thus, under the independent source doctrine, objects that have been illegally seized may be re-seized even if the illegal seizure came first in a sequence of events leading to the legal seizure. *Murray*, 487 U.S. at 542. Even though "[t]o determine whether the warrant was independent of the illegal[ity], one must ask whether it would have been sought even if what actually happened had not occurred," *id.*, the fuller question is whether the warrant resulted from "exploitation of that illegality or instead by means sufficiently distinguishable [from it]." *Wong Sun*, 371 U.S. at 488 (internal quotation marks and citation omitted).

Courts analyzing the second prong of the independent doctrine test have often looked to context to determine what motivated law enforcement officers, particularly to determine what else they had learned in their investigation. See *Johnson*, 994 F.2d at 987 (finding that the second prong of the independent doctrine test was satisfied because "there was probable cause for the warrant to issue, and the agents had good reason to want to review the tapes[; i]n fact, the only reason the agents failed to apply for a warrant prior to listening to the tapes was their mistaken belief that they were entitled to do so"); see also *United States v. Stabile*, 633 F.3d 219, 245 (3d Cir. 2011) (illegal viewing of child pornography videos on the defendant's computer did not prompt subsequent application for warrant to search his computers for child pornography because "it would be impossible or inconceivable that" the warrant application would not have been made in light of a detective's lawful viewing of "lurid file names indicative of child pornography") (internal quotation marks and citation omitted). Here, the context informs the conclusion that the independent doctrine test is satisfied.

The stipulation and other evidence before the Court establish that the FBI was not motivated to seek a warrant by

any information gleaned from the first search of Nayyar's computer, but instead was motivated to seek a warrant in order to obtain evidence relevant to the pending charges against Nayyar and the months-long FBI investigation, as well as to buttress the legal authority for the search the FBI had begun before anyone from the FBI saw any of the contents of Nayyar's computer. Moreover, the FBI, and the Government, did not profit in any way from the initial search of the computer, and would be placed in a substantially worse position than it otherwise would have occupied if the computer evidence is suppressed based on an initial search for which the FBI mistakenly, but reasonably, thought it had received consent from someone with access to the computer. See *Murray*, at 542 ("The independent source doctrine . . . [rests] upon the policy that, while the government should not profit from its illegal activity, neither should it be placed in a worse position than it would otherwise have occupied."); *Johnson*, 994 F.2d at 987 (finding that the independent source doctrine applied where the government began reviewing evidence under a mistaken belief it could do so).

The FBI's investigation of Nayyar began in July 2009. See *Stip.*, Ex. G ¶ 8. During that month, Nayyar told a confidential FBI source that he had access to sniper rifles,



which he could sell to the source, and also had access to armor penetrating sniper bullets and night-vision goggles. See Stip., Ex. G ¶ 9(b). In August 2009, Nayyar offered to sell Uzis to the source and sold to the source a handgun and a box of hollow-point ammunition, in packaging that said "For Law Enforcement Use Only, Not For Retail Sale." Stip., Ex. G ¶ 9(d)-(f). Nayyar also showed the source another gun that he refused to sell, saying it was for his personal use, and told the source that he was traveling to Atlanta to obtain items for the source from his contact in Atlanta. See Stip., Ex. G ¶ 9(d)-(e), (h).

In September 2009, Nayyar told the source that the night-vision goggles and bulletproof vests they had discussed were available to be picked up, and provided the source with a three-page computer printout purporting to be specifications for night-vision goggles. See Stip., Ex. G ¶ 9(k). During the investigation, the FBI recorded more than a dozen meetings between Nayyar and the CI, which lasted, in total, about 20 hours. See Tr. 12. In the course of the investigation Nayyar provided the CI with, in addition to the materials described above, an arms catalog from a weapons manufacturer, which contained descriptions and specifications for weapons ranging from high-powered rifles to rocket-propelled grenades, printouts



of specifications for M-18 mines, and an armor plate for use in bulletproof vests. GX 3, GX 53, GX 48.

Searches of Nayyar's apartment and the adjacent apartment of his mother on September 24, 2009, the day of Nayyar's arrest, yielded several boxes of ammunition (both hollow point and full metal jacket), GX 1, 8, 9, 10, 11, the original version of the arms catalog he provided to the CI, GX 3, several rounds of spent ammunition that appeared to have been used to test a bullet proof vest or armor plate, GX 2, printouts of specification for a Russian-made helicopter, GX 12, correspondence with a Romania-based weapons manufacturer regarding Nayyar's attempts some years earlier to acquire weapons, GX 5, 6, and several other related documents, including plane tickets to Romania. GX 4A, 4B.

Following his arrest, Nayyar admitted that he agreed to sell a truck to the CI knowing that the truck would be used by Hizballah, and admitted that he discussed with the CI the number of missiles the truck could carry. See Stip., Ex. G ¶ 12(a)-(b). Nayyar also admitted that he sold a handgun and ammunition to the source with the understanding that the gun and ammunition would be provided to the "Mullah" of Hizballah.

Stip., Ex. G ¶ 12(c). Nayyar further admitted that he had researched how to manufacture bullet proof vests in the past and that he was hoping to start a bullet proof vest manufacturing business and provide those vests to Hizballah. Stip., Ex. G ¶ 2(d). In October 2009, Nayyar was indicted for conspiring to provide, and providing, material support to Hizballah, conspiring to make, and making, a contribution of funds, goods or services to Hizballah, and illegal possession of a firearm and ammunition. See Indictment.

Agent Kelley first took steps to examine Nayyar's computer on November 2, 2009, see Stip. ¶ 12, after all the evidence just described had been obtained and a week after Nayyar was indicted on the charges just described. The parties have stipulated that when he began to search the computer, Agent Kelley "[s]pecifically . . . was looking to obtain evidence related to a printout about night-vision goggles that Nayyar had provided to the confidential source prior to Nayyar's arrest . . . ." Stip. ¶ 23. The search terms he used reflected both that specific goal and the charges in the case, as he searched only for "night vision goggles" and "M-16." Stip. ¶ 23(a)-(d), (1).

As set forth above, after Agent Kelley discovered images that might be child pornography, he stopped his search and spoke with AUSA Buckley. See Stip. ¶¶ 23(k), 24. During that conversation and one that followed, AUSA Buckley explored the legal authority for the search that Agent Kelley had begun. See Stip. ¶¶ 24, 25. Upon learning the relevant facts, AUSA Buckley instructed Agent Kelley to halt his search, expressed concerns about the legal authority for the search and told Agent Kelley that, "in order to cure any potential deficiency in the legal authority" for the search he had begun, the FBI should obtain a search warrant. Stip. ¶ 25(b). AUSA Buckley also said that if, in the course of the renewed search, the FBI identified confirmed images of child pornography, it would need to obtain a new search warrant specific to the child pornography. *Id.* In October 2010 the FBI sought a search warrant that permitted it to search for evidence, fruits and instrumentalities of violations of the statutes underlying the indictment against Nayyar (except for the gun possession charge). Stip., Ex. G at 26 (Attachment B).

Nayyar has contended that AUSA Buckley inquired regarding the legal basis for the search "in light of the potential contraband on the laptop." Nayyar Br. at 13. Nayyar

points to the fact that "[w]hen the Government resumed the process of searching the laptop after the search warrant had been obtained, the initial focus was on child pornography," in support of his claim that "the images Kelley found during the initial, unlawful search were exactly what spurred the Government to pursue a search warrant." Nayyar Br. at 16 (footnote omitted). Nothing in the Stipulation of Facts supports a conclusion that AUSA Buckley's inquiry about the legal basis for the search was in any way focused on the potential contraband. The Stipulation states that, during his conversation with AUSA Buckley, "Agent Kelly did not describe the images that he had seen nor did he provide copies of the images to AUSA Buckley." Stip. ¶ 24. Had the suspected child pornography images motivated the search warrant application, the FBI would have sought a warrant that permitted it to search for and seize evidence related to those images, such as addresses, address books, mailing lists and supplier lists related to the possession, production and receipt of child pornography.

The searches conducted by the FBI to which Nayyar cites were conducted on December 9 and 10, 2010. See Stip. ¶ 39. A few weeks earlier, on October 27, Nayyar, through his defense attorney, had pressed the Government for a copy of his

computer's hard drive, see Stip. ¶ 32, and on December 3 Nayyar's counsel provided Agent Kelly with a hard drive that was to be used to make a complete copy of the computer for discovery purposes. See Stip. ¶ 36. On December 7, two days before the FBI began the searches Nayyar cites,

representatives from CART contacted Agent Kelley to inform him that they were unable to make a discovery copy of the computer for defense counsel's review. Specifically, because there was reason to believe that the hard drive contained potential images of child pornography, CART would not duplicate the computer for production to defense counsel out of a concern that doing so would violate federal laws related to the distribution and transportation of child pornography.

Stip. ¶ 37. And on December 8, one day before the FBI began the searches Nayyar cites, arrangements were made to permit defense counsel to review the computer at the U.S. Attorney's Office or the FBI. Stip. ¶ 38. The following month the FBI followed up and had an agent review the suspected images to see if they should be treated as child pornography. Stip. ¶ 44.

The FBI's search for child pornography to which Nayyar cites was an effort to determine how discovery of



the computer could be made - whether it required the more cumbersome procedure of review at government offices for a computer that actually contained child pornography, rather than the procedure that the parties had contemplated of providing the defense with its own copy of the computer, which would be more efficient for both the FBI and the defense. Nayyar's claim that the search for child pornography shows that the images of suspected child pornography found by Agent Kelley when he first reviewed the computer "were exactly what spurred the Government to pursue a search warrant," Nayyar Br. at 16, is unsupported.

Instead, the FBI sought to search for and seize evidence relevant to the serious pending charges against, and the FBI's substantial and longstanding investigation of, Nayyar. In doing so, as Nayyar concedes, see Nayyar Br. at 16 n.8, the FBI relied on nothing it had seen during the initial search. See *United States v. Hanhardt*, 155 F. Supp.2d at 851 (the nature of information submitted in support of the search warrant application "is also relevant to the motivational inquiry") (citation omitted). What motivated the decision to obtain a search warrant was a desire to obtain evidence relevant to the longstanding investigation of and pending charges against Nayyar

Nayyar and, specifically, AUSA Buckley's "concerns about Ms. Nayyar's ability to consent to a search" of the computer, and his desire to "cure any potential deficiency in the legal authority (i.e., Ms. Nayyar's consent form) previously relied upon by the FBI to commence the forensic examination." Stip. ¶ 25(b).

In this case, as in *Johnson*, "the agents had good reason to want to review" the items at issue. 994 F.2d at 987. Likewise, in both cases, "the only reason the agents failed to apply for a warrant prior" to beginning their search "was their mistaken belief that they were entitled to" conduct the search. *Id.*; see Stip. ¶ 24(b) ("AUSA Buckley asked Agent Kelley upon what legal authority he had relied in conducting his initial search of the forensic image of Laptop #2, to which Agent Kelley responded that he had relied upon Ex. B, i.e., the 'Consent to Search Computer(s)' form signed by Ms. Nayyar."). Again, in this case, as in *Johnson*, once someone else (in *Johnson* the judge, here the prosecutor) "expressed reservation about the legality of the review," the agents realized that a warrant was necessary and sought one. *Id.*; see also *Hanhardt*, 155 F.Supp.2d at 851 (decision to seek warrant to search briefcase searched illegally

earlier was prompted by appellate ruling suppressing the evidence). And in this case, as in *Johnson*,

Whether the agents made their mistake in good faith is not relevant to this inquiry. What is key is the fact that their error did not result in the government obtaining evidence it would not otherwise have obtained. The government would have acquired the evidence on the tapes without the agents' mistaken prior review of the tapes, since the warrant application was prompted not by the prior review but by the obvious relevance of the tapes and the district court's indication that a warrant was necessary.

994 F.2d at 987. While the agents in *Johnson* had heard all of the tapes they later sought a search warrant to review, 994 F.2d at 982, in this case the agent stopped his review of the computer after seeing very little of what was on it. See *United States v. Simmonds*, No. 5:13-CR-42, 2014 WL 1706296, at \*11 (D. Vt. Apr. 29, 2014), *aff'd*, 641 F. App'x 99 (2d Cir. 2016) ("As in *Johnson*, the government's search warrant application here was prompted not by the prior review of Defendant's cell phone, but instead by the obvious relevance of the cell phone to the conspiracy charge against Defendant and Defendant's argument in his motion to suppress that the initial search of the cell phone was unlawful. The instant case thus falls squarely within *Johnson*."); see also *United States v. Howe*, No. 09-

CR-6076L, 2011 WL 2160472, at \*14 (W.D.N.Y. May 27, 2011) (finding the independent source exception applied where warrant application contained no information obtained through warrantless searches and government represented that "it decided to apply for the federal warrant, not because of information learned from the warrantless searches, but because it had not realized until that time that although a state warrant had been issued, it authorized only a search of [defendant's] residence, and not the laptop" at issue).

The FBI here mistakenly thought it had consent to search Nayyar's computer, searched the computer briefly and then, when advised that it should obtain a warrant, did so. There is no "evidence to which instant objection is made [that] has been come at by exploitation of that illegality." *Wong Sun*, 371 U.S. at 88. Nothing seen during the initial warrantless search was introduced as an individual exhibit at trial; nor was any of it the subject of any testimony or argument at trial. See Stip. ¶ 23 (e)-(j). The initial search was not a "confirmatory search." What prompted the application for the search warrant was the longstanding investigation of, and pending charges



against, Nayyar, coupled with the prosecutor's concerns about the consent to search that had been provided. See *Johnson*, 994 F.2d at 987. The independent source exception to the exclusionary rule applies to this situation; the evidence obtained from the computer was appropriately admitted.

### **Conclusion**

Based upon the facts and conclusions set forth above, Nayyar waived his right to challenge the computer evidence, Mrs. Nayyar's consent was invalid, and the independent source doctrine applies. Nayyar's motion for a mistrial and to suppress the computer evidence is denied.

It is so ordered.

New York, NY  
November 18, 2016

  
\_\_\_\_\_  
ROBERT W. SWEET  
U.S.D.J.